CEFMS and Electronic Signatures

2.1 Smartcard Security.

When receiving a card and PIN, it is very important to follow the security procedures listed below

2.1.1 Always keep the card in a safe place when it is not being used. A wallet or a locked drawe r is the best place to keep the card.

2.1.2 Sign the PIN envelope before opening to validate that it has not been tampered with prior to receipt.

2.1.3 Return the top sheet of the envelope to the dSO issuing the password.

2.1.4 Memorize the PIN then destroy the second sheet of the envelope. Do not throw it away without shredding the document first.

2.1.5 Do not write the PIN down or give it to another User.

2.1.6 If the PIN is revealed to another User, immediately contact the dSO for a new card. If the card is lost or stolen, immediately contact the dSO. The dSO will deactivate the card so that it can no longer be used. A new card and PIN will be issued.

2.1.7 A lost card or compromised PIN is a serious security issue since the User can be held responsible for transactions authorized with the missing or compromised card.

Contact The dSO Immediately If A Card Is Lost Or Pin Compromised.

2.2 Deactivate Smartcard Due to Employment Termination.

Smartcards will be deactivated when a user leaves an organization. The card must be returnedto the dSOs so it can be deactivated to prevent the user from signing any additional messages. The flag in the database will be set to indicate that although the user is no longer active, the signatures generated by the user may still be validated.

2.3 Compromised PIN.

Smartcards will be deactivated when a PIN is compromised or the user suspects a PIN is compromised. The smartcard must be promptly returned to the dSOs. The user is not deleted from the database so that signatures generated by the user may still be used to verify messages previously signed by the user. The user will receive a new smartcard and PIN.

2.4 Lost Smartcard.

Smartcards will be deactivated when a card is lost. The dSOs must be notified immediately that a card was lost. The database will be updated to set the flag to indicate that although the card is no longer active, the signatures previously generated by the user may still be verified. The database will be updated with the date a smartcard is deactivated. Any signature generated after this date may not be verified. The user will receive a new smartcard and PIN.

2.5 Security Violations.

2.5.1 If a user sees or knows of unauthorized use of smartcards or PINs, i.e., sharing, notify the individual's supervisor for appropriate disciplinary action.

2.5.2 If a user finds an unattended computer with a smartcard in the smartcard reader, attempt to log them off CEFMS and remove the smartcard. If you cannot log them off, remove the smartcard and take to the individual's supervisor. Inform the supervisor of the incident so that he/she may take appropriate disciplinary action.

2.5.3 If you find a smartcard, take it to your supervisor so he/she may decide if disciplinary action is necessary. The user may have already reported the loss of the smartcard to a dSO.

2.5.4 If you find a PIN written down, notify the supervisor for appropriate disciplinary action. PINs should be memorized and not written down for unauthorized viewing.